



MoGua

JLWCS 1.1.7.APK 分析报告



APP名称:

JLWCS

包名:	com.lq.nblg
域名线索:	23条
URL线索:	29条
邮箱线索:	0条
分析日期:	2025年10月2日
分析平台:	摸瓜APK反编译平台

文件名: hsjl-117-1.apk
文件大小: 59.54MB
MD5值: dab2a611254670a606f6b10828a69fac
SHA1值: b7005645e8edaf67a1c5f844511459e12ff7c484
SHA256值: 55ef503bf53e58c956d809fc75286bba9d38dd80d80f2019350b4c444c297ee2

i APP 信息

App名称: JLWCS
包名: com.lq.nblg
主活动Activity: com.unity3d.player.UnityPlayerActivity
安卓版本名称: 1.1.7
安卓版本: 1

🔍 域名线索

域名	服务器信息
openmobile.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
appsupport.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
	IP: 60.28.215.27 所属国家: China 地区: Tianjin

cgi.connect.qq.com	城市: Tianjin 纬度: 39.142181 经度: 117.176102
graph.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
pingma.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
android.bugly.qq.com	IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
app.qq.com	IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
huatuocode.huatuo.qq.com	没有服务器地理信息.
up.sdk.mob.com	IP: 180.188.26.28 所属国家: China 地区: Zhejiang 城市: Taizhou

	纬度: 28.666668 经度: 121.349998
mta.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
p.share.mob.com	没有服务器地理信息.
long.open.weixin.qq.com	IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
fusion.qq.com	IP: 116.130.228.157 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.utag.mob.com	没有服务器地理信息.
api.u.mob.com	没有服务器地理信息.
	IP: 141.144.196.217

mta.oa.com	所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
www.mob.com	IP: 180.188.26.28 所属国家: China 地区: Zhejiang 城市: Taizhou 纬度: 28.666668 经度: 121.349998
api.weixin.qq.com	IP: 116.128.170.42 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
rqd.uu.qq.com	IP: 60.28.219.32 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
open.weixin.qq.com	IP: 140.207.176.25 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
cgi.qplus.com	没有服务器地理信息.
	IP: 123.6.25.75 所属国家: China 地区: Henan

qzs.qq.com	城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
------------	--

 URL线索

URL信息	Url所在文件
http://qzs.qq.com/open/mobile/login/qzsjump.html?sdkv=3.3.0.lite&display=mobile	cn/sharesdk/tencent/qq/a.java
http://app.qq.com/detail/com.tencent.mobileqq?autodownload=1&norecommend=1&rootvia=opensdk	cn/sharesdk/tencent/qq/a.java
https://graph.qq.com/oauth2.0/m_authorize?response_type=token&client_id=	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com/user/get_simple_userinfo	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com/oauth2.0/m_authorize?response_type=token&client_id=	cn/sharesdk/tencent/qzone/b.java
https://graph.qq.com/user/get_simple_userinfo	cn/sharesdk/tencent/qzone/b.java
https://graph.qq.com/photo/upload_pic	cn/sharesdk/tencent/qzone/b.java
https://graph.qq.com	cn/sharesdk/tencent/qzone/b.java
http://p.share.mob.com/tags/getTagList	cn/sharesdk/framework/authorize/f.java
https://)	cn/sharesdk/framework/b/a.java
https://api.weixin.qq.com/sns/oauth2/access_token	cn/sharesdk/wechat/utils/g.java

https://api.weixin.qq.com/sns/oauth2/refresh_token	cn/sharesdk/wechat/utils/g.java
https://api.weixin.qq.com/sns/userinfo	cn/sharesdk/wechat/utils/g.java
http://api.u.mob.com	com/mob/MobUser.java
http://www.mob.com/about/policy\	com/mob/commons/dialog/d.java
http://www.mob.com/about/policy	com/mob/commons/dialog/d.java
http://api.utag.mob.com/conf	com/mob/commons/utag/TagRequester.java
http://api.utag.mob.com/bdata	com/mob/commons/utag/UserTager.java
http://up.sdk.mob.com	com/mob/commons/filesys/FileUploader.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApiml.java
http://qzs.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApiml.java
http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApiml.java
http://qzs.qq.com	com/tencent/open/SocialApiml.java
https://graph.qq.com/cgi-bin/qunopensdk/unbind	com/tencent/open/SocialOperation.java
https://graph.qq.com/cgi-bin/qunopensdk/check_group	com/tencent/open/SocialOperation.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utils/f.java

http://cgi.qplus.com/report/report	com/tencent/open/utlis/k.java
https://huatuocode.huatuo.qq.com	com/tencent/open/b/d.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuiid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
https://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
https://graph.qq.com/oauth2.0/me	com/tencent/connect/UnionInfo.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/BaseApi.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/common/BaseApi.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/auth/a.java
https://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/user/user_login_statis	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/v3/user/get_info	com/tencent/connect/auth/AuthAgent.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1\$s&from=%2\$s&isOpenAppID=1	com/tencent/connect/share/QQShare.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1\$s&from=%2\$s&isOpenAppID=1	com/tencent/connect/share/QzoneShare.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java

http://www.mob.com/about/policy>http://www.mob.com/about/policy	摸瓜V1引擎
http://www.mob.com	摸瓜V1引擎
http://www.mob.com/about/policy>http://www.mob.com/about/policy.lf	摸瓜V1引擎
https://github.com/rust-lang/rust/issues/39364assertion	lib/arm64-v8a/discord_game_sdk.so
https://github.com/rust-lang/rust/issues/39364	lib/arm64-v8a/discord_game_sdk.so

邮箱线索

手机线索

手机号	所在文件
19222222222	com/mob/commons/a/h.java

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=CN, ST=ZJ, L=HZ, O=BLKK, OU=BLKK, CN=Simon
签名算法: rsassa_pkcs1v15
有效期自: 2022-04-25 03:50:33+00:00
有效期至: 2077-01-26 03:50:33+00:00
发行人: C=CN, ST=ZJ, L=HZ, O=BLKK, OU=BLKK, CN=Simon
序列号: 0x5a35cffd

哈希算法: sha256
md5值: 33b7664b6c80176842c4b66dd7fbf0a3
sha1值: 7552bf20e001f452abcd25129b78758786d9888e
sha256值: adf7a0c19f6c9d2b53fc4003873261689fe706bc189c8bcd1c5e6d78c3587f54
sha512值: b61dac2bd46f9f887b4e5f2a543645fd3b5598811d087e8682101852b453ea8558ea56974c05191a50b341c844290e811d735c190f52395451c6328aaa1e5b98
公钥算法: rsa
密钥长度: 2048
指纹: 0ea4b471e8ea1add01e89c9dc34fefba079ba74262194143ffdc2a28c7b34be6

硬编码敏感信息

可能的敏感信息
"PASSWORD" : "Password"
"USERNAME" : "Username"
"mobcommon_authorize_dialog_accept" : "接受"
"mobcommon_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/about/policy。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobcommon_authorize_dialog_reject" : "拒绝"
"mobcommon_authorize_dialog_title" : "服务授权"
"mobdemo_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/about/policy。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobdemo_authorize_dialog_title" : "服务授权"
"ssdk_cmcc_auth" : "手机认证服务由中国移动提供"
"ssdk_cmcc_login_one_key" : "本机号码一键登录"

"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"PASSWORD" : "암호"
"USERNAME" : "사용자 이름"
"mobdemo_authorize_dialog_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see detailshttp://www.mob.com/about/policy.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject."
"mobdemo_authorize_dialog_title" : "service authority"
"ssdk_cmcc_auth" : "Provided by China Mobile"
"ssdk_cmcc_login_one_key" : "PhoneNum Login"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"
"PASSWORD" : "Adgangskode"
"USERNAME" : "Brugernavn"
"PASSWORD" : "パスワード"
"USERNAME" : "ユーザー名"
"PASSWORD" : "Passwort"
"USERNAME" : "Nutzername"
"PASSWORD" : "パスワード"

PASSWORD : 密码
"USERNAME" : "用户名"
"PASSWORD" : "Mật khẩu"
"USERNAME" : "Tên đăng nhập"
"PASSWORD" : "Wachtwoord"
"USERNAME" : "Gebruikersnaam"
"PASSWORD" : "Mot de passe"
"USERNAME" : "Nom d'utilisateur"
"PASSWORD" : "Contraseña"
"USERNAME" : "Nombre de usuario"
"PASSWORD" : "Parola d'ordine"
"USERNAME" : "Nome utente"
"PASSWORD" : "Senha"
"USERNAME" : "Nome de usuário"
"PASSWORD" : "пароль"
"USERNAME" : "имя пользователя"
"PASSWORD" : "Lösenord"
"USERNAME" : "Användarnamn"

"PASSWORD" : "密碼"
"USERNAME" : "用戶名"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息

android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.unity3d.player.UnityPlayerActivity	Schemes: hsjl://, Hosts: com.lq.nblg,
cn.sharesdk.tencent.qq.ReceiveActivity	Schemes: tencent101570008://,